TRAITE DE COOPERATION EN MATIERE DE BREVETS

Rec'd PCT/PTO 19 JUL 2004

10 MARS 2004 10/501823

PCT

Expéditeur : L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

Destinataire :

Jeune, Pascale
FRANCE TELECOM T&I/PIV/PI
38-40, rue du Général Leclerc
92794 Issy Moulineaux Cedex 9
FRANCE

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(règle 71.1 du PCT)

Date d'expédition *(jour/mois/année)*	10.03.2004
Référence du dossier du déposant ou du mandataire: 04134	**NOTIFICATION IMPORTANTE**

Demande internationale No.	Date du dépôt international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR 03/00112	15.01.2003	17.01.2002

Déposant: FRANCE TELECOM et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **NOTIFICATION IMPORTANTE**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Il est signalé au déposant que l'article 33(5) stipule que les critères de nouveauté, d'activité inventive et d'application industrielle tels que définis à l'article 33(2) à (4) ne servent qu'aux fins de l'examen préliminaire international et que "tout État contractant peut appliquer des critères additionnels ou différents afin de décider si, dans cet État, l'invention est brevetable ou non" (voir également l'article 27(5)). De tels critères additionnels peuvent par exemple avoir rapport à des exceptions à la brevetabilité ainsi qu'à des exigences concernant l'exposé suffisant de l'invention, la clarté des revendications et leur fondement sur la description.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international

Office européen des brevets - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tél. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Fonctionnaire autorisé

Emery, C

Tel. +31 70 340-2848

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale No. PCT/FR 03/00112	Date du dépôt international *(jour/mois/année)* 15.01.2003	Date de priorité *(jour/mois/année)* 17.01.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant FRANCE TELECOM et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 3 feuilles.

3. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants : (104)

   - I ☒ Base de l'opinion
   - II ☐ Priorité
   - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
   - IV ☐ Absence d'unité de l'invention
   - V ☒ Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
   - VI ☐ Certains documents cités
   - VII ☐ Irrégularités dans la demande internationale
   - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
19.07.2003	10.03.2004
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Dujardin, C N° de téléphone +31 70 340-2840

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL Demande internationale n° PCT/FR 03/00112

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale *(les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17))* :

Description, Pages

1-12 telles qu'initialement déposées

Revendications, No.

1-6 reçue(s) le 27.01.2004 avec lettre du 22.01.2004

Dessins, Feuilles

1/5-5/5 telles qu'initialement déposées

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, nos :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-6
	Non:	Revendications	
Activité inventive	Oui:	Revendications	1-6
	Non:	Revendications	
Possibilité d'application industrielle	Oui:	Revendications	1-6
	Non:	Revendications	

2. Citations et explications

   voir feuille séparée

Concernant le point V

1) Il est fait référence au document suivant:
D1: WO 00 08610 A (MICROSOFT CORP) 17 février 2000 (2000-02-17)

2) Le document D1 (les références entre parenthèses s'appliquent à ce document), qui est considéré comme l'état de la technique le plus proche, décrit un procédé cryptographique (page 14, ligne 14 - page 16, ligne 6; figures 1 et 2) mis en oeuvre par une carte à puce d'un ensemble de cartes à puces appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce comprenant un moyen de mémorisation dans lequel sont mémorisés une clé secrète, un identifiant de la première entité propriétaire de la carte à puce et un identifiant de la carte à puce, et comprenant un moyen de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète, procédé comprenant les étapes qui consistent:

- avant tout calcul par le moyen de calcul de la puce, à lire par la puce dans un moyen de mémorisation d'une seconde entité ("point of transaction unit" 24 dans la figure 1) une liste d'identifiants de cartes à puce, cette liste étant liée à chaque état attribué à chacune des cartes à puces par une troisième entité ("card issuer" 22 dans la figure 1).
- à comparer par la puce l'identifiant mémorisé dans le moyen de mémorisation de la puce et le contenu de la liste, pour autoriser ou interdire tout calcul du moyen de calcul en fonction du résultat de la comparaison.

L'objet de la revendication 1 diffère donc de ce procédé cryptographique connu en ce que

A) l'identifiant utilisé pour la comparaison identifie la première entité propriétaire de la carte et non la carte elle-même.
B) la liste d'identifiants se présente sous forme intégrale
C) l'entité dans le moyen de mémorisation de laquelle la puce lit la liste d'identifiants avant tout calcul par le moyen de la puce est la même que l'entité qui attribue un état à chacune des premières entités.

L'objet de la revendication 1 est donc nouveau (article 33(2) PCT).

Le problème principal que la présente invention se propose de résoudre peut être

considéré comme étant d'éviter une possible fraude pendant l'intervalle de temps qui sépare le dernier transfert de la liste de la troisième entité vers la deuxième entité et la lecture de la liste dans la mémoire de la deuxième entité.

La solution de ce problème proposée dans la revendication 1 de la présente demande est considérée comme impliquant une activité inventive (article 33(3) PCT), et ce pour les raisons suivantes:

La caractéristique C mentionnée ci-dessus du procédé cryptographique selon la revendication 1 n'est pas connue et ne découle pas d'une manière évidente de l'état de la technique. Cette caractéristique est de plus combinée dans la revendication 1 avec deux autres caractéristiques (les caractéristiques A et B ci-dessus) et il ne serait par conséquent pas évident pour l'homme du métier d'obtenir un procédé cryptographique selon la revendication 1 à partir des enseignements des documents de l'état de l'art.

3) Les revendications 2-5 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

4) La revendication 6 ne satisfait pas aux conditions requises à l'article 6 PCT, dans la mesure où l'objet (à savoir une carte à puce) pour lequel une protection est recherchée n'est pas clairement défini. La revendication 6 tente de définir certaines caractéristiques de cet objet en fonction de caractéristiques d'éléments extérieurs à cet objet (à savoir une liste d'identifiants dans un moyen de mémorisation d'une seconde entité; voir page 14, ligne 34 à page 15, ligne 3). La revendication 6 devrait donc être clarifiée.

Un système cryptographique comprenant à la fois la carte à puce décrite dans la revendication 6, ainsi que la "seconde entité" mentionnée dans la revendication 6, comporterait des caractéristiques correspondantes à celles du procédé de la revendication 1. Les arguments utilisés dans le cas du procédé de la revendication 1, au paragraphe 2) ci-dessus, seraient donc aussi applicables à ce système cryptographique et celui-ci remplirait, par conséquent, les conditions visées à l'article 33(1)-(3) PCT.

REVENDICATIONS

1. Procédé cryptographique mis en œuvre par une carte (30) à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce (31) comprenant un moyen (32) de mémorisation dans lequel sont mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte (30) à puce et comprenant un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète, caractérisé en ce qu'il comprend les étapes qui consistent :
   - avant tout calcul par le moyen (33) de calcul de la puce (31) de la carte (30) à puce, à lire (2) par la puce (31) dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,
   - à comparer (3) par la puce (31) l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen (33) de calcul en fonction du résultat de la comparaison.

2. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) n'appartient pas à la liste.

3. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à non révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) appartient à la liste.

4. Procédé cryptographique selon l'une des revendications 1 à 3, comprenant en outre les étapes qui consistent :

REVENDICATIONS

1. Procédé cryptographique mis en œuvre par une carte (30) à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce (31) comprenant un moyen (32) de mémorisation dans lequel sont mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte (30) à puce et comprenant un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète, caractérisé en ce qu'il comprend les étapes qui consistent :
   - avant tout calcul par le moyen (33) de calcul de la puce (31) de la carte (30) à puce, à lire (2) par la puce (31) dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,
   - à comparer (3) par la puce (31) l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen (33) de calcul en fonction du résultat de la comparaison.

2. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) n'appartient pas à la liste.

3. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à non révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) appartient à la liste.

4. Procédé cryptographique selon l'une des revendications 1 à 3, comprenant en outre les étapes qui consistent :

- en même temps que la lecture (2) de la liste, à lire (10) une signature de cette liste par la puce (31) dans le moyen de mémorisation de la seconde entité, la signature ayant été préalablement calculée par un moyen de calcul de la seconde entité,
- avant autorisation (5) par la puce de tout calcul du moyen (33) de calcul, à vérifier (11) par la puce (31) la validité de la signature.

5. Procédé cryptographique selon l'une des revendications 1 et 2, comprenant en outre les étapes qui consistent :
   - en même temps que la lecture (2) de la liste, à lire (12) des signatures des identifiants de la liste par la puce (31) dans le moyen de mémorisation de la seconde entité, chaque identifiant ayant donné lieu à une signature préalablement calculée par un moyen de calcul de la seconde entité,
   - en même temps que la lecture (2) de la liste, à lire (13, 14) par la puce (31) dans le moyen de mémorisation de la seconde entité, une valeur du nombre d'identifiants listés dans cette liste ainsi qu'une signature de cette valeur, la valeur et sa signature ayant été préalablement calculées par un moyen de calcul de la seconde entité,
   - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de calcul, à vérifier (16, 17) par la puce (31) la validité de chacune des signatures,
   - à compter (15) par la puce (31) le nombre d'identifiants contenus dans la liste lue,
   - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de calcul, à vérifier (18) l'égalité entre la valeur du compteur et la valeur lue.

6. Carte (30) à puce pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 5, caractérisée en ce qu'elle (30) est équipée d'une puce (31) qui comprend au moins :
   - un moyen (32) de mémorisation d'une clé secrète et d'un identifiant d'une première entité propriétaire de la carte à puce,
   - un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète,
   - un moyen (34) de lecture pour lire une liste d'identifiants, de premières entités propriétaires d'une carte à puce, sous forme intégrale dans un moyen

de mémorisation d'une seconde entité, via un réseau de télécommunication, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,

- un moyen (35) de comparaison entre l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et le contenu de la liste, pour autoriser ou interdire tout calcul du moyen (33) de calcul en fonction du résultat de la comparaison.